



UNITED STATES PATENT AND TRADEMARK OFFICE

MN
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/663,478	09/15/2003	James R. Trethewey	42P17784	2896
59796 7590 06/26/2007 INTEL CORPORATION c/o INTELLEVATE, LLC P.O. BOX 52050 MINNEAPOLIS, MN 55402				
			EXAMINER HA, LEYNNA A	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 06/26/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/663,478

Applicant(s)

TRETHERWEY ET AL.

Examiner

LEYNNA T. HA

Art Unit

2135

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 April 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,5-13,15-25,27 and 28 is/are pending in the application.
- 4a) Of the above claim(s) 4,14 and 26 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,5-13,15-25,27 and 28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3, 5-13, 15-25, and 27-28 are pending.
Claims 4, 14, and 26 have been cancelled.
2. This is a Non-Final rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 1-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moles, et al. (US 6,505,048) and further in view of Hertz, et al. (US 6,571,279).**

As per claim 1:

Moles discloses a method comprising:

receiving a request from a requestor for a location property associated with a location of a computer system; and **(col.2, lines 10-15 and col.6, lines 21-22; The computer system can broadly be given as a wireless mobile station as disclosed by Moles (col.4, lines 48-53). Moles teach the**

operator is the claimed requestor who is doing the requesting. The requestor of Moles may also be a user of wireless mobile station.)

determining whether a privacy preference associated with the requestor has been specified; and **(col.2, lines 24-26 and col.2, line 66 – col.3, line 2; Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted.)**

if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request.

Moles discloses the user can send the information in privacy flag record to another output device (col.9, lines 57-60) and suggests setting location privacy flag (col.11, lines 5-6). However, Moles did not clearly suggest if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request.

The claimed if privacy preference associated with the requestor has not been specified can broadly interpret as a requestor cannot gain access because the privacy preference is not given or identified. Thus, would make sense to request from the user a privacy preference associated with the requestor as claimed if the privacy preference was not already given or specified.

Hertz, et al. discloses the beacon capability of the mobile subscriber stations can be used to identify a user, and using this subscriber identification information, to locate and fetch a user profile for the identified subscriber (col.4, lines 28-31) and can be used to access a variety of information in a user-dependent profile (col.6, lines 41-42). Hertz discusses each user with a user identifier has one or more location identifiers LID, which are unique identifiers associated with a specific user terminal device and which can be used to determine a location of the user terminal device (col.7, lines 63-66). Hertz further discloses advertiser and other users can access to user profiles based upon certain guidelines that dictate the terms and conditions by which an individual grants another individual access privileges to gain access to his/her profile and introduce to the user based upon features/credentials constituting the user profiles of the requestor. These guidelines constitute part of the requestor's privacy policy (col.13, lines 29-35). Automatic matching techniques notifies users of other users that are located in or near the same vicinity and match the desired profile conditions, as consistent with the privacy policies of users, e.g. for purposes of notification, request for electronic introduction and/or delivery of dynamic messages may be subject to conditions set forth by the user (col.13, lines 36-46). Hertz discloses access control criteria dictating profile access and reachability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). The above explanation shows the profile and privacy policies are

Art Unit: 2135

assigned or conditioned by users where the conditions and policy of a requestor has to match or have certain criteria when attempting to introduce with another user (col.14, lines 15-18 and col.15, lines 3-11). If the requestor does not meet to the profile and privacy profile conditioned by the user (col.15, line 66 – col.16, line 8), then it is obvious the requestor is either not allowed to communicate or the requestor has not been identified with this particular user. Thus, this obviously suggests the claimed privacy preference associated with the requestor has not been specified. Hertz discloses access controls may be used to enable (or restrict) the ability of an explicitly identified user to be automatically identified upon his/her entering the proximity of the requestor (col.15, lines 16-20). In addition, Hertz discloses vendors and advertisers are likely to request access to certain user profile data relating to user location information to gain access (col.16, lines 8-11) where user profiles are assigned and rules dictating the user's disclosure policy with respect to which user or user type may gain access to which information (col.15, lines 22-45). Hertz obviously suggests the privacy preference associated with the requestor has not been specified and that requesting a privacy preference associated with the requestor from the user because the user is able to restrict the ability to automatically identify himself to the requestor.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a

privacy preference associated with the requestor from the user in response to receiving the request because access control may be used to enable or restrict the ability of an explicitly identified user to be automatically identified upon entering the proximity of the requestor which forces the requests for privacy policies from users so as to ensure the utmost security of the user profile data (col.15, lines 3-45 and col.18, lines 56-65).

As per claim 2: See Moles on col.2, lines 36-39 and col.2, line 66 – col.3, line 2; discussing if a privacy preference associated with the requestor has been specified, applying the specified preference to determine whether to provide the location property to the requestor.

As per claim 3: See Moles on col.2, lines 24-26 and 61-63 and col.7, lines 14-18; discussing preventing the location property from being provided to the requestor if the privacy preference specifies that the location property is to be kept private, and providing the location property to the requestor if the privacy preference specifies that the location property is to be disclosed to the requestor.

As per claim 4: Cancelled.

As per claim 5: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55; discussing requesting includes providing a pop-up dialog box.

As per claim 6: See Moles on col.6, lines 57-65; discussing providing a pop-up dialog box includes enabling a user to selectively enable and disable privacy for individual location properties.

As per claim 7:

Moles discloses a method comprising:

enabling a user to selectively enable and disable location-aware computing; and **(col.2, lines 34-48)**

preventing a location property from being provided to a requestor if the user has disabled location-aware computing; and **(col.2, lines 24-26 and 61-63 and col.7, lines 14-18)**

if the user has enabled location-aware computing, determining whether a privacy preference associated with the requestor has been specified; and

if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving a request from the requestor for a location property associated with a computing system.

Moles discloses the user can send the information in privacy flag record to another output device (col.9, lines 57-60) and suggests setting location privacy flag (col.11, lines 5-6). However, Moles did not clearly suggest if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request.

The claimed if privacy preference associated with the requestor has not been specified can broadly interpret as a requestor cannot gain access because the privacy preference is not given or identified. Thus, would make sense to

request from the user a privacy preference associated with the requestor as claimed if the privacy preference was not already given or specified.

Hertz, et al. discloses the beacon capability of the mobile subscriber stations can be used to identify a user, and using this subscriber identification information, to locate and fetch a user profile for the identified subscriber (col.4, lines 28-31) and can be used to access a variety of information in a user-dependent profile (col.6, lines 41-42). Hertz discusses each user with a user identifier has one or more location identifiers LID, which are unique identifiers associated with a specific user terminal device and which can be used to determine a location of the user terminal device (col.7, lines 63-66). Hertz further discloses advertiser and other users can access to user profiles based upon certain guidelines that dictate the terms and conditions by which an individual grants another individual access privileges to gain access to his/her profile and introduce to the user based upon features/credentials constituting the user profiles of the requestor. These guidelines constitute part of the requestor's privacy policy (col.13, lines 29-35). Automatic matching techniques notifies users of other users that are located in or near the same vicinity and match the desired profile conditions, as consistent with the privacy policies of users, e.g. for purposes of notification, request for electronic introduction and/or delivery of dynamic messages may be subject to conditions set forth by the user (col.13, lines 36-46). Hertz discloses access control criteria dictating profile access and reachability of the user may be controlled accordingly based

Art Unit: 2135

upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). The above explanation shows the profile and privacy policies are assigned or conditioned by users where the conditions and policy of a requestor has to match or have certain criteria when attempting to introduce with another user (col.14, lines 15-18 and col.15, lines 3-11). If the requestor does not meet to the profile and privacy profile conditioned by the user (col.15, line 66 – col.16, line 8), then it is obvious the requestor is either not allowed to communicate or the requestor has not been identified with this particular user. Thus, this obviously suggests the claimed privacy preference associated with the requestor has not been specified. Hertz discloses access controls may be used to enable (or restrict) the ability of an explicitly identified user to be automatically identified upon his/her entering the proximity of the requestor (col.15, lines 16-20). In addition, Hertz discloses vendors and advertisers are likely to request access to certain user profile data relating to user location information to gain access (col.16, lines 8-11) where user profiles are assigned and rules dictating the user's disclosure policy with respect to which user or user type may gain access to which information (col.15, lines 22-45). Hertz obviously suggests the privacy preference associated with the requestor has not been specified and that requesting a privacy preference associated with the requestor from the user because the user is able to restrict the ability to automatically identify himself to the requestor.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request because access control may be used to enable or restrict the ability of an explicitly identified user to be automatically identified upon entering the proximity of the requestor which forces the requests for privacy policies from users so as to ensure the utmost security of the user profile data (col.15, lines 3-45 and col.18, lines 56-65).

As per claim 8: See Moles on col.6, lines 57-61 and col.9, lines 51-60; discusses enabling the user to selectively enable and disable location-aware computing includes providing an option during basic input/output system configuration to enable and disable location-aware computing.

As per claim 9: See Moles on col.2, lines 36-39 and col.2, line 66 – col.3, line 2; discusses setting a location privacy setting bit in response to the user selectively enabling or disabling location-aware computing.

As per claim 10: See Moles on col.2, lines 65-67 and Hertz on col.10, lines 24-35; discusses setting the location privacy setting bit includes setting a bit in BIOS memory.

As per claim 11: See Moles on col.2, lines 10-41 and col.6, lines 57-61; discusses receiving a request for the location property from the requestor, and

Art Unit: 2135

querying the location privacy setting bit to determine whether location-aware computing is enabled or disabled.

As per claim 12: See Moles on col.9, lines 50-60; discusses setting and querying are performed using Advanced Configuration and Power Interface (ACPI)-based techniques.

As per claim 13:

Moles discloses a machine-accessible medium storing instructions that, when executed by a machine, cause the machine to:

in response to receiving a request from a requestor for a location property, determine whether a privacy preference associated with the requestor has been specified; and **(col.2, lines 10-40 and col.2, line 66 – col.3, line 2; Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted.)**

if a privacy preference associated with the requestor has been specified **(col.2, lines 34-48)**, applying the privacy preference to determine whether to provide or withhold the location property; and **(col.6, lines 57-61 and col.9, lines 27-31 and 50-54)**

if a privacy preference associated with the requestor has not been specified, request that the privacy preference be specified in response to receiving the request.

Moles discloses the user can send the information in privacy flag record to another output device (col.9, lines 57-60) and suggests setting location privacy

flag (col.11, lines 5-6). However, Moles did not clearly suggest if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request.

The claimed if privacy preference associated with the requestor has not been specified can broadly interpret as a requestor cannot gain access because the privacy preference is not given or identified. Thus, would make sense to request from the user a privacy preference associated with the requestor as claimed if the privacy preference was not already given or specified.

Hertz, et al. discloses the beacon capability of the mobile subscriber stations can be used to identify a user, and using this subscriber identification information, to locate and fetch a user profile for the identified subscriber (col.4, lines 28-31) and can be used to access a variety of information in a user-dependent profile (col.6, lines 41-42). Hertz discusses each user with a user identifier has one or more location identifiers LID, which are unique identifiers associated with a specific user terminal device and which can be used to determine a location of the user terminal device (col.7, lines 63-66). Hertz further discloses advertiser and other users can access to user profiles based upon certain guidelines that dictate the terms and conditions by which an individual grants another individual access privileges to gain access to his/her profile and introduce to the user based upon features/credentials constituting the user profiles of the requestor. These guidelines constitute part of the

requestor's privacy policy (col.13, lines 29-35). Automatic matching techniques notifies users of other users that are located in or near the same vicinity and match the desired profile conditions, as consistent with the privacy policies of users, e.g. for purposes of notification, request for electronic introduction and/or delivery of dynamic messages may be subject to conditions set forth by the user (col.13, lines 36-46). Hertz discloses access control criteria dictating profile access and reachability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). The above explanation shows the profile and privacy policies are assigned or conditioned by users where the conditions and policy of a requestor has to match or have certain criteria when attempting to introduce with another user (col.14, lines 15-18 and col.15, lines 3-11). If the requestor does not meet to the profile and privacy profile conditioned by the user (col.15, line 66 – col.16, line 8), then it is obvious the requestor is either not allowed to communicate or the requestor has not been identified with this particular user. Thus, this obviously suggests the claimed privacy preference associated with the requestor has not been specified. Hertz discloses access controls may be used to enable (or restrict) the ability of an explicitly identified user to be automatically identified upon his/her entering the proximity of the requestor (col.15, lines 16-20). In addition, Hertz discloses vendors and advertisers are likely to request access to certain user profile data relating to user location information to gain access (col.16, lines 8-11) where user profiles are assigned

Art Unit: 2135

and rules dictating the user's disclosure policy with respect to which user or user type may gain access to which information (col.15, lines 22-45). Hertz obviously suggests the privacy preference associated with the requestor has not been specified and that requesting a privacy preference associated with the requestor from the user because the user is able to restrict the ability to automatically identify himself to the requestor.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request because access control may be used to enable or restrict the ability of an explicitly identified user to be automatically identified upon entering the proximity of the requestor which forces the requests for privacy policies from users so as to ensure the utmost security of the user profile data (col.15, lines 3-45 and col.18, lines 56-65).

As per claim 14: Cancelled.

As per claim 15: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55; discloses provide a pop-up dialog box to request the privacy preference.

As per claim 16: See Moles on col.2, line 66 – col.3, line 2; discloses determine whether the machine is enabled for location-aware computing.

As per claim 17: See Moles on col.7, lines 14-45 and Hertz on col.13, lines 24-46 and col.15, lines 3-45; discloses if the machine is not enabled for location-

aware computing, preventing the machine from providing the requested location property regardless of whether the privacy preference has been specified and, if specified, regardless of the contents of the privacy preference.

As per claim 18:

Moles discloses a method comprising:

in response to receiving a request for a location property from a requestor, determining whether a computer system is enabled for location-aware computing; **(col.2, lines 10-26 and col.2, line 66 – col.3, line 2; Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted.)**

if the computer is enabled for location-aware computing, determining whether a privacy preference associated with the requestor has been specified; **(col.2, lines 36-40)**

if the privacy preference associated with the requestor has been specified, applying the privacy preference to determine whether to provide the location property; and **(col.2, lines 34-48 and col.9, lines 27-31 and 50-54)**

if the privacy preference associated with the requestor has not been specified, requesting the privacy preference associated with the requestor **(col.6, lines 57-61) in response to receiving the request.**

Moles discloses the user can send the information in privacy flag record to another output device (col.9, lines 57-60) and suggests setting location privacy

flag (col.11, lines 5-6). However, Moles did not clearly suggest if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request.

The claimed if privacy preference associated with the requestor has not been specified can broadly interpret as a requestor cannot gain access because the privacy preference is not given or identified. Thus, would make sense to request from the user a privacy preference associated with the requestor as claimed if the privacy preference was not already given or specified.

Hertz, et al. discloses the beacon capability of the mobile subscriber stations can be used to identify a user, and using this subscriber identification information, to locate and fetch a user profile for the identified subscriber (col.4, lines 28-31) and can be used to access a variety of information in a user-dependent profile (col.6, lines 41-42). Hertz discusses each user with a user identifier has one or more location identifiers LID, which are unique identifiers associated with a specific user terminal device and which can be used to determine a location of the user terminal device (col.7, lines 63-66). Hertz further discloses advertiser and other users can access to user profiles based upon certain guidelines that dictate the terms and conditions by which an individual grants another individual access privileges to gain access to his/her profile and introduce to the user based upon features/credentials constituting the user profiles of the requestor. These guidelines constitute part of the

requestor's privacy policy (col.13, lines 29-35). Automatic matching techniques notifies users of other users that are located in or near the same vicinity and match the desired profile conditions, as consistent with the privacy policies of users, e.g. for purposes of notification, request for electronic introduction and/or delivery of dynamic messages may be subject to conditions set forth by the user (col.13, lines 36-46). Hertz discloses access control criteria dictating profile access and reachability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). The above explanation shows the profile and privacy policies are assigned or conditioned by users where the conditions and policy of a requestor has to match or have certain criteria when attempting to introduce with another user (col.14, lines 15-18 and col.15, lines 3-11). If the requestor does not meet to the profile and privacy profile conditioned by the user (col.15, line 66 – col.16, line 8), then it is obvious the requestor is either not allowed to communicate or the requestor has not been identified with this particular user. Thus, this obviously suggests the claimed privacy preference associated with the requestor has not been specified. Hertz discloses access controls may be used to enable (or restrict) the ability of an explicitly identified user to be automatically identified upon his/her entering the proximity of the requestor (col.15, lines 16-20). In addition, Hertz discloses vendors and advertisers are likely to request access to certain user profile data relating to user location information to gain access (col.16, lines 8-11) where user profiles are assigned

and rules dictating the user's disclosure policy with respect to which user or user type may gain access to which information (col.15, lines 22-45). Hertz obviously suggests the privacy preference associated with the requestor has not been specified and that requesting a privacy preference associated with the requestor from the user because the user is able to restrict the ability to automatically identify himself to the requestor.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request because access control may be used to enable or restrict the ability of an explicitly identified user to be automatically identified upon entering the proximity of the requestor which forces the requests for privacy policies from users so as to ensure the utmost security of the user profile data (col.15, lines 3-45 and col.18, lines 56-65).

As per claim 19: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55; discloses requesting the privacy preference comprises providing a pop-up dialog box.

As per claim 20: See Moles on col.2, lines 65-67 and Hertz on col.10, lines 24-35; discloses determining whether a computer system is enabled for location-aware computing comprises determining a value stored in a location privacy setting in basic input/output system (BIOS) memory.

As per claim 21: See Moles on col.6, lines 56-57; discloses enabling a user to enable and disable location-aware computing through a BIOS configuration routine.

As per claim 22: See Moles on col.9, lines 9-34 and 50-60; discloses using WMI/ACPI instrumentation techniques to set and determine the value stored in the location privacy setting.

As per claim 23:

Moles discloses a system comprising:

- a bus to communicate information; **(col.5, lines 21-22)**

- a processor coupled to the bus; **(col.4, lines 51-57)**

- a memory coupled to the bus to store information; **(col.2, lines 65-66)**

- an antenna coupled to the bus to receive a signal to indicate a location of the system; and **(col.2, lines 5-15)**

- a machine-accessible storage medium storing instructions that, when executed by the processor, cause the system to:

- in response to receiving a request for a location property associated with the system from a requestor, determine whether a privacy preference associated with the requestor has been specified; and **(col.2, lines 10-40 and col.2, line 62 – col.3, line 2; Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted.)**

if a privacy preference has been specified, apply the privacy preference to determine whether to provide the requested location property. **(col.2, lines 34-48 and col.9, lines 27-31 and 50-54)**

if a privacy preference associated with the requestor has not been specified, request that the privacy preference be specified in response to receiving the request.

Moles discloses the user can send the information in privacy flag record to another output device (col.9, lines 57-60) and suggests setting location privacy flag (col.11, lines 5-6). However, Moles did not clearly suggest if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request.

The claimed if privacy preference associated with the requestor has not been specified can broadly interpret as a requestor cannot gain access because the privacy preference is not given or identified. Thus, would make sense to request from the user a privacy preference associated with the requestor as claimed if the privacy preference was not already given or specified.

Hertz, et al. discloses the beacon capability of the mobile subscriber stations can be used to identify a user, and using this subscriber identification information, to locate and fetch a user profile for the identified subscriber (col.4, lines 28-31) and can be used to access a variety of information in a user-dependent profile (col.6, lines 41-42). Hertz discusses each user with a user identifier has one or more location identifiers LID, which are unique identifiers

associated with a specific user terminal device and which can be used to determine a location of the user terminal device (col.7, lines 63-66). Hertz further discloses advertiser and other users can access to user profiles based upon certain guidelines that dictate the terms and conditions by which an individual grants another individual access privileges to gain access to his/her profile and introduce to the user based upon features/credentials constituting the user profiles of the requestor. These guidelines constitute part of the requestor's privacy policy (col.13, lines 29-35). Automatic matching techniques notifies users of other users that are located in or near the same vicinity and match the desired profile conditions, as consistent with the privacy policies of users, e.g. for purposes of notification, request for electronic introduction and/or delivery of dynamic messages may be subject to conditions set forth by the user (col.13, lines 36-46). Hertz discloses access control criteria dictating profile access and reachability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). The above explanation shows the profile and privacy policies are assigned or conditioned by users where the conditions and policy of a requestor has to match or have certain criteria when attempting to introduce with another user (col.14, lines 15-18 and col.15, lines 3-11). If the requestor does not meet to the profile and privacy profile conditioned by the user (col.15, line 66 – col.16, line 8), then it is obvious the requestor is either not allowed to communicate or the requestor has not been identified with this particular user.

Art Unit: 2135

Thus, this obviously suggests the claimed privacy preference associated with the requestor has not been specified. Hertz discloses access controls may be used to enable (or restrict) the ability of an explicitly identified user to be automatically identified upon his/her entering the proximity of the requestor (col.15, lines 16-20). In addition, Hertz discloses vendors and advertisers are likely to request access to certain user profile data relating to user location information to gain access (col.16, lines 8-11) where user profiles are assigned and rules dictating the user's disclosure policy with respect to which user or user type may gain access to which information (col.15, lines 22-45). Hertz obviously suggests the privacy preference associated with the requestor has not been specified and that requesting a privacy preference associated with the requestor from the user because the user is able to restrict the ability to automatically identify himself to the requestor.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request because access control may be used to enable or restrict the ability of an explicitly identified user to be automatically identified upon entering the proximity of the requestor which forces the requests for privacy policies from users so as to ensure the utmost security of the user profile data (col.15, lines 3-45 and col.18, lines 56-65).

Art Unit: 2135

As per claim 24: See Moles on col.2, line 66 – col.3, line 2; discloses the machine-accessible storage medium further stores instructions that, when executed by the processor, cause the system to determine whether the system is enabled for location-aware computing.

As per claim 25: See Moles on col.2, lines 65-67 and Hertz on col.10, lines 24-35; discloses the memory includes a basic input/output system (BIOS) memory and wherein determining whether the system is enabled for location-aware computing includes determining a value stored in a location in the BIOS memory.

As per claim 26: See Moles on col.7, lines 14-45 and Hertz on col.13, lines 24-46 and col.15, lines 3-45; discloses storing instructions that, when executed by the processor, cause the system to request the privacy preference associated with the requestor if it is determined that the privacy preference associated with the requestor has not been specified.

As per claim 27: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55; discloses requesting the privacy preference includes providing a pop-up dialog box.

As per claim 28: See Moles on col.4, lines 45-65; discloses the requestor is one of a client application and a location-based service.

Response to Arguments

4. Applicant's arguments, filed 4/19/2007, with respect to the rejection(s) of claim(s) 1, 7, 13, 18, 23 under Moles have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Moles and Hertz, et al.

Claims 1, 7, 13, 18, 23 is currently amended to recite if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request.

The claimed "if privacy preference associated with the requestor has not been specified" can broadly interpret as a requestor cannot gain access because the privacy preference is not given or identified. Thus, would make sense to request from the user a privacy preference associated with the requestor as claimed if the privacy preference was not already given or specified. Regarding pg.12 of applicant's argument, Examiner does not agree that the claimed "if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request" with applicant's interpretation is asking the user to set a privacy preference in response to a request. Claims 1, 7, 13, 18, 23 broadly is limited to requesting a privacy

Art Unit: 2135

preference from the user but does not further limit the user to "set" a privacy preference. The claimed invention does not go beyond requesting such as the user responding to this request by transmitting the privacy preference back to the requestor nor setting any privacy preference.

Mole does not discuss if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request. Thus, Hertz is brought forth to teach this limitation.

Hertz discloses access control criteria dictating profile access and reachability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). Hertz discloses access controls may be used to enable (or restrict) the ability of an explicitly identified user to be automatically identified upon his/her entering the proximity of the requestor (col.15, lines 16-20). In addition, Hertz discloses vendors and advertisers are likely to request access to certain user profile data relating to user location information to gain access (col.16, lines 8-11) where user profiles are assigned and rules dictating the user's disclosure policy with respect to which user or user type may gain access to which information (col.15, lines 22-45). The above explanation shows the profile and privacy policies are assigned or conditioned by users where the conditions and policy of a requestor has to match or have certain criteria when attempting to introduce with another user (col.14, lines 15-18 and col.15, lines 3-11). If the

Art Unit: 2135

requestor does not meet to the profile and privacy profile conditioned by the user (col.15, line 66 – col.16, line 8), then it is obvious the requestor is either not allowed to communicate or the requestor has not been identified with this particular user. Thus, this obviously suggests the claimed privacy preference associated with the requestor has not been specified and that requesting a privacy preference associated with the requestor from the user because the user is able to restrict the ability to automatically identify himself to the requestor.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user in response to receiving the request because access control may be used to enable or restrict the ability of an explicitly identified user to be automatically identified upon entering the proximity of the requestor which forces the requests for privacy policies from users so as to ensure the utmost security of the user profile data (col.15, lines 3-45 and col.18, lines 56-65).

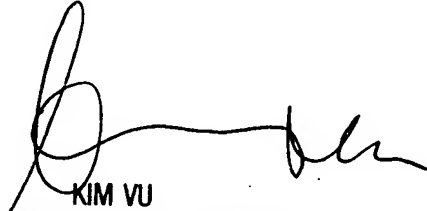
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100